Jeff D. Friedman (173886)
HAGENS BERMAN SOBOL SHAPIRO LLP
715 Hearst Avenue, Suite 202
Berkeley, CA 94710
Telephone: (510) 725-3000
Facsimile: (510) 725-3001
jefff@hbsslaw.com

Steve W. Berman, *pro hac vice* (application pending)
Thomas E. Loeser (202724)
HAGENS BERMAN SOBOL SHAPIRO LLP
1918 Eighth Avenue, Suite 3300
Seattle, WA 98101
Telephone: (206) 623-7292
Facsimile: (206) 623-0594
steve@hbsslaw.com
toml@hbsslaw.com

*Attorneys for Plaintiffs and the Proposed Class*

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

| | |
|---|---|
| NANCY L. MANCIAS, CHRISTI L. DEL NAGRO, COREY ABELS, ANDREW LAWHERN, PATRICE DAVIS, individually and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>TARGET CORPORATION, a Minnesota Corporation,<br><br>Defendant. | No.<br><br>CLASS ACTION COMPLAINT<br><br>**DEMAND FOR JURY TRIAL** |

## TABLE OF CONTENTS

## I. INTRODUCTION

1. A national retail chain with Point-of-Sale ("POS") computer systems that store credit card and ATM card information must ensure that its customers' personal and financial information is safeguarded from theft. When a data breach affecting at least 70 million customers occurs, a national retail chain must *immediately and accurately* notify its customers to prevent such customers from incurring financial losses, losses of time, and inconvenience as a result of the actual or threatened fraudulent use of stolen personal and financial information. This lawsuit stems from Target's failure to follow these two simple rules.

2. Target is the second largest discount retail store system in the United States. Its estimated annual sales exceed $73.8 billion. Beginning on or about November 17, 2013, and continuing until December 15, 2013, the POS computer network that processes transactions for all Target Corporation ("Target") retail stores was breached by unknown attackers. The breach resulted in the largest theft of personal and financial information in history and affected at least 40 million credit card and ATM accounts and the personal and financial information of at least 70 million individuals.

3. The massive Target POS data breach could have been prevented. As early as 2007 Target was specifically warned by a data security expert about the possibility of a POS data breach, it was told how to prevent such a breach, and it was even told that failure to act could possibly result in the compromise of as many as 58 million charge accounts. Even though Target described the security expert's suggestions as "good ideas," on information and belief it did not implement them. Further, Target likely did not comply with the industry-standard PCI Data Security Standard, under which Target may have prevented, and at least would have sooner discovered, the POS data breach.

4. To make matters worse, Target did not promptly disclose the POS data breach and did not notify victims of the POS data breach in a reasonable or timely manner. Quite the contrary, Target did not disclose the POS data breach at all until the day after Brian Krebs, a computer security and cybercrime blogger, reported it on his blog on December 18, 2013, and the POS data breach became widely reported in the press.

5. As a result of the Target POS data breach, the credit card and ATM card accounts – with the associated PINs – of 40 million accounts, as well as the personal information of 70 million Target customers, have been exposed to fraud and these customers have been harmed as a result. On January 10, 2014, nearly two months after the breach began, Target disclosed that *in addition to charge card information for 40 million accounts*, customer names, addresses, phone numbers and email addresses of 70 million customers were also stolen in the POS data breach. Harm to victims of the Target POS data breach includes: fraudulent charges on their accounts; time and expense related to: (a) finding fraudulent charges; (b) cancelling and reissuing cards; (c) credit monitoring and identity theft prevention; (d) imposition of withdrawal and purchase limits on compromised accounts; and (e) the general nuisance and annoyance of dealing with all these issues resulting from the Target POS data breach in the weeks leading up to the end-of-year holiday season. Plaintiffs seek to remedy these harms, and prevent their future occurrence, on behalf of themselves and all victims of the Target POS data breach.

## II. JURISDICTION

6. This Court has diversity jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). At least one Plaintiff and Defendant are citizens of different states. The amount in controversy exceeds $5 million and there are more than 100 putative class members.

7. This Court has personal jurisdiction over the Defendant because Defendant is licensed to do business in California or otherwise conducts business in California.

8. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because unlawful practices are alleged to have been committed in this federal judicial district, property involved in a Plaintiff's claim is in this district, a Plaintiff resides in this district and Defendant regularly conducts business in this district.

## III. PARTIES

9. Plaintiff Nancy Mancias resides in San Rafael, California. On November 28, 2013, she used her ATM card and associated PIN number to make a purchase at the Target store in Novato, California. Ms. Mancias believed that Target would maintain her personal and financial information in a reasonably secure manner and provided her information to Target on that basis.

Had Plaintiff known that Target would not maintain her information in a reasonably secure manner, she would not have made a purchase at Target using her ATM card and PIN.

10. Plaintiff Andrew Lawhern resides in Tacoma, Washington. On December 3, 2013, he used his debit card and associated PIN at the Target store located at 3310 S. Meridian, Puyallup, Washington. Mr. Lawhern believed that Target would maintain his personal and financial information in a reasonably secure manner and provided his information to Target on that basis. Had Plaintiff known that Target would not maintain his information in a reasonably secure manner, he would not have made a purchase at Target using his ATM card and PIN.

11. Plaintiff Christi L. Del Nagro resides in Seattle, Washington. On December 5 and December 16, 2013, she used her debit card and associated PIN at the Target store located in Seattle, Washington. Ms. Del Nagro believed that Target would maintain her personal and financial information in a reasonably secure manner and provided her information to Target on that basis. Had Plaintiff known that Target would not maintain her information in a reasonably secure manner, she would not have made a purchase at Target using her ATM card and PIN.

12. Plaintiff Corey Abels resides in Aurora Colorado. On December 2, 3, and 9, 2013, he used his debit card and associated PIN at the Target store located in Aurora, Colorado. Mr. Abels believed that Target would maintain his personal and financial information in a reasonably secure manner and provided his information to Target on that basis. Had Plaintiff known that Target would not maintain his information in a reasonably secure manner, he would not have made a purchase at Target using his ATM card and PIN.

13. Plaintiff Patrice ("Trish") Davis resides in Goodyear, Arizona. On December 5 and December 6, 2013, she used her debit card and associated PIN at the Target store located in Goodyear, Arizona. Ms. Davis believed that Target would maintain her personal and financial information in a reasonably secure manner and provided her information to Target on that basis. Had Plaintiff known that Target would not maintain her information in a reasonably secure manner, she would not have made a purchase at Target using her ATM card and PIN.

14. Defendant Target Corporation is a Minnesota corporation, headquartered in Minneapolis, Minnesota. Target is one of the largest discount retailers in the United States with almost 1,800 retail stores.

## IV. FACTS

### A. Target Collects its Customers' Personal Information

15. Target is the second-largest discount retailer in the United States and is currently ranked 36th on the "Fortune 500" list of top US companies.[1] Target advertises and sells discounted merchandise directly to millions of consumers through its 1,797 retail store in the United States.

16. When a customer makes a purchase at a Target retail stores using a credit or debit card, including Target's branded REDcard, Target collects information related to that card including the card holder name, the account number, expiration date, card verification value (CVV), and PIN for ATM/debit cards. It stores this information in its Point-of-Sale ("POS") system and transmits this information to a third party for completion of the payment. Target also collects and stores customer names, mailing addresses, phone numbers, and email addresses.

17. Target recognizes that its customers' personal and financial information is highly sensitive and must be protected. According to Target's December 11, 2013, Privacy Policy, "[b]y interacting with Target, [customers] consent to use of information that is collected or submitted as described in this privacy policy." Target states:

> We maintain administrative, technical and physical safeguards to protect your personal information. When we collect or transmit sensitive information such as a credit or debit card number, we use industry standard methods to protect that information.

18. The PCI Data Security Standard ("PCI DSS") is an industry standard for large retail institutions that accept credit card and debit card transactions. The standard consists of 12 general requirements:

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

[1] http://money.cnn.com/magazines/fortune/fortune500/2013/snapshots/2303.html?iid=F500_fl_list.

3. Protect stored data

4. Encrypt transmission of cardholder data and sensitive information across public networks

5. Use and regularly update anti-virus software

6. Develop and maintain secure systems and applications

7. Restrict access to data by business need-to-know

8. Assign a unique ID to each person with computer access

9. Restrict physical access to cardholder data

10. Track and monitor all access to network resources and cardholder data

11. Regularly test security systems and processes

12. Maintain a policy that addresses information security

19. PCI DSS is intended to:

> Build and maintain a secure network; protect cardholder data; ensure the maintenance of vulnerability management programs; implement strong access control measures; regularly monitor and test networks; and ensure the maintenance of information security policies.[2]

20. On December 23, 2013, USA Today reported that Target was likely not PCI compliant. The article stated:

> Target's massive databreach took place just a few weeks before a set of payment card industry standards – known as PCI DSS 3.0 – were scheduled to go into effect. CyberTruth asked Nick Aceto, technology director at software vendor CardConnect, to supply some clarity.
>
> **CT:** What does this latest databreach tell us about the efficacy of PCI?
>
> **Aceto:** We can't say definitely that this breach is a failure of Target's PCI compliance, but based on what Target has said, it's very hard to believe that they were even PCI 2.0 compliant at the time of the breach.
>
> A reason for thinking this is that the attack, involving an enormous amount of data, went on essentially unnoticed for 18 days. How were they not watching the network?
>
> One of the PCI DSS requirements is that you monitor your logs and firewalls every day, looking for unusual activity. This monitoring

[2] https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

> involves file integrity checks and changes to critical systems files. What's more – the chapter 6 software development life cycle requires the secure distribution and verification of payment applications.
>
> Unusual activity isn't always abnormal, but the point of PCI is to monitor and verify that all activity is normal, while not letting distractions – like busy shopping days Black Friday and Cyber Monday, on which the breach occurred – detract from the monitoring effort.[3]

21. On information and belief, Target did not follow or properly implement the PCI Data Security Standard or any other equally effective industry standard to protect customers' personal and financial information.

**B. Vulnerability of Corporate POS Systems Was Made Known to Target Years Before this Data Breach**

22. On August 27, 2007, Dr. Neal Krawetz of Hacker Factor Solutions[4] publicly disclosed a white paper titled "Point-of-Sale Vulnerabilities" (the "White Paper").[5] The White Paper Abstract describes its content as follows:

> Point-of-Sale (POS) systems provide the initial interface for credit card transactions. While the communications between POS systems have been hardened through the use of cryptography and a variety of authentication techniques, the devices themselves provide virtually no security. Few POS systems implement best practices for handling sensitive information, such as the Visa standards for credit card management. This document describes common risks to credit card users due to POS systems.[6]

---

[3] http://www.usatoday.com/story/cybertruth/2013/12/23/qa-pci-rules-could-help-stymie-target-data-thieves/4179941/.

[4] The Hackerfactor website states:

> Neal Krawetz earned his Ph.D. in Computer Science from Texas A&M University and Bachelors degree in Computer and Information Science from the University of California, Santa Cruz. In 2002, he founded Hacker Factor Solutions (www.hackerfactor.com) where he specializes in non-classical computer forensics, online profiling, and computer security. His research into anti-anonymity technologies combines fields as vast as ergonomics and child development to artificial intelligence and theoretical biophysics. He is the author of three books and numerous articles, and is a popular speaker at local and national conferences. His work experience spans small startup companies, academic and university environments, and large Fortune-100 corporations.

[5] Available in the public domain at: http://www.hackerfactor.com/papers/cc-pos-20.pdf.

[6] *See id.*, p. 4.

23. The White Paper describes as background how between January and March 2006, thousands of credit card customers received letters containing replacement cards and stating that their card information may have been compromised. "[T]he potentially compromised information was everything on the card: name, card number, expiration date, possibly the CVV2 (number on the back of the card), and possibly the PIN code." The background section discusses a Bank of America announcement in February 2006 that an unnamed retailer (possibly OfficeMax) had compromised some 200,000 credit card numbers. It further reported that the POS provider for OfficeMax may have been the source of the compromise. The background section concludes:

> Although the person responsible for the compromise is unknown, the retailer is inconclusive, and the details of the compromise continually change, the method for conducting the compromise is likely due to a lack of POS security. Furthermore, the unsafe storage of credit card information in POS systems is not limited to FTS or OfficeMax; it impacts nearly **every** POS vendor and retailer. This vulnerability was discussed with Verifone between 1992 and 1993 – this is a fourteen-year-old attack method.[7]

24. The White Paper then provides a detailed description of the typical POS system and its components, including "5.2.2 Lax security processes" and "5.3 Security up for Auction." Importantly, the White Paper goes on to describes POS "Branch Servers" and how their vulnerability could result in the compromise of millions of credit card accounts.[8]

25. Presciently, ***the 2007 White Paper uses Defendant Target as an example of the potential ramifications of a POS data breach at a major retailer***. It estimates that as many as 58 million card accounts could be compromised if Target's POS system was compromised. For a paper written over six years *before* the data breach at issue here, Dr. Krawetz' estimate using assumed transaction frequency and data storage times is remarkably close.[9]

26. In his conclusion for the White Paper, Dr. Krawetz specifically notes:

> Point-of-sale terminals and branch servers store credit card information in ways that are no longer secure enough. These vulnerabilities are not limited to any single POS vendor; they pose a fundamental hole in the entire POS market. It seems that nearly

---

[7] *Id.* (emphasis in original).

[8] *See id.* at pp. 10-12.

[9] *See id.* at pp. 11-12.

> every POS provider is vulnerable, including Verifone, Fujitsu Transaction Solutions, Retalix, Hypercom, Autostar, Innovax, JDA, JPMA, NCR, StoreNext, IBM, and Systech. Similarly, these vulnerabilities impact all retailers that use these systems, including (but not limited to) OfficeMax, BestBuy, Circuit City, ***Target***, Wal-Mart, REI, Staples, Nordstrom, and Petco. The amount of vulnerability varies between retailers and their implementations. But in general, if a credit card is not required to return a product, or the product can be returned at any store, then the retailer likely has a serious vulnerability.[10]

27. Dr. Krawetz summarizes the vulnerable aspects of the POS architecture, including Branch Servers and closes:

> Even though other sightings have occasionally surfaced, the February 9th [2006] announcement showed the first big vendor being publicly hit with this problem. This compromise was not the first, it is unlikely to be the last, and it certainly will not be the biggest. ***It is only a matter of time before a national branch server at a large retailer is compromised***.[11]

28. On or about August 7, 2007, a Target employee responsible for Target's POS system acknowledged receipt of the White Paper and requested permission to provide it to other Target employees. The Target employee described Dr. Krawetz suggestions as "good ideas."

29. Dr. Krawetz' website logs the web domains that download copies of his documents. A domain registered to Target Corporation downloaded 17 copies of the White Paper between August, 2007 and May, 2013. Search terms that led to downloads of the White Paper to the Target domain as late as May, 2013, included "POS vulnerability."

30. On information and belief, Target did not implement the suggestions in the White Paper.

**C. The POS Data Breach and Target's Failure to Promptly and Accurately Notify**

31. Sometime between November 27, 2013, and December 15, 2013, hackers gained access to Target's data network and stole the credit and debit card information for about 40 million Target shoppers and the personal information of 70 million. According to initial reports, the

---

[10] *Id.* p. 14 (emphasis added).

[11] *Id.* p. 15 (emphasis added).

breach affected only customers of Target's brick-and-mortar U.S. store locations and not those who shopped at Target's online stores.[12]

32. Security experts said the timing of the breach corresponds with a recent surge of stolen credentials being offered for sale on underground cybercrime forums. "We started to detect that something was afoot on December 11th when [we] detected a massive increase – 10 - 20x – in availability of high-value stolen cards on black-market sites," read a blog post from security vendor Easy Solutions. "Nearly every bank and [credit union] in the US seems to be affected."[13]

33. On December 19, 2013, Target issued a press release confirming that unknown attackers were able to gain unauthorized access to Target's payment card data.[14] According to Target, the unknown data thieves stole data including customer names, card expiration dates, and the card verification value (CVV), also known as the card security code (CSC).[15]

34. Target posted a notification to customers of the data breach on its corporate website, not on its general consumer website. This decreased the likelihood that Target shoppers would read the notification and was perhaps intended to minimize the adverse effects of the data breach on Target sales during the busy holiday shopping period. Furthermore, Target did not help customers protect their personal and financial information, but instead told customers to do it themselves. Its notice told customers:

> You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect fraud, be sure to report it immediately to your financial institutions. In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft.

---

[12] http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/.

[13] http://www.informationweek.com/security/attacks-and-breaches/target-breach-10-facts/d/d-id/1113228.

[14] https://corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca.

[15] *Id.*

35. Target initially stated and told customers that PIN numbers were not compromised by the breach.[16] This was false and deceptive. On December 27, 2013, Target finally disclosed that PIN data was stolen during the breach. Nevertheless, even then, Target deceptively downplayed the PIN data theft, including by only telling customers that "strongly encrypted PIN data was removed from our system during the data breach incident," "your debit card account has not been compromised," and "PINs are safe and secure."[17] Despite Target's statements, experts believe the stolen PIN data may reasonably be decrypted and fraudulently used.[18]

36. On January 10, 2014, Target again changed its story concerning the POS data breach. Target stated that in addition to the 40 million compromised credit and ATM accounts, 70 million customer names, mailing addresses, phone numbers and email addresses were also stolen in the POS data breach.[19]

37. News of the breach was first reported on December 18 by computer security blogger Brian Krebs on his blog, krebsonsecurity.com. In breaking the story, Krebs confirmed with independent fraud analysts that Target had been breached after they were able to buy a number of stolen card accounts from a well-known "card shop" – an online store advertised in cybercrime forums as a place where thieves can reliably buy stolen credit and debit cards.

38. Investigators believe that the data was obtained via software installed on the POS machines at Target stores that customers used to swipe their credit cards when paying for merchandise.[20] Through this software, the thieves were able to steal the name, account number, expiration date, and CVV for each card that was swiped.

---

[16] *Id.*; https://corporate.target.com/about/payment-card-issue.aspx?ref= sr_shorturl_paymentcardresponse (click on "e-mail to guests (sent on 12.20.13)").

[17] https://corporate.target.com/about/payment-card-issue.aspx?ref=sr_ shorturl_ paymentcardresponse (click on "pin update (posted on 12.27.13)").

[18] http://www.npr.org/2013/12/29/258009006/targets-word-may-not-be-enough-to-keep-your-stolen-pins-safe; *see also* http://www.nbcnews.com/video/ nightly-news/53927467/#53927467.

[19] http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance.

[20] http://www.cbsnews.com/news/target-confirms-massive-credit-debit-card-data-breach/.

39. The type of data stolen – also known as "track data" – allows crooks to create counterfeit cards by encoding the information onto any card with a magnetic stripe.[21] Thus, the thieves could take the credit card information and create a fake credit card that could be swiped and used to make purchases as if it were the real credit card. Additionally, the thieves could reproduce stolen debit cards and use them to withdraw cash from ATMs.[22] With the additional personal information that Target disclosed was stolen on January 10, 2014, thieves could seek to change credit card billing addresses and create completely fictional credit accounts in unsuspecting victim's names.

40. As reported at Informationweek.com, according to the Payment Card Industry Data Security Standard (PCI-DSS), merchants like Target are required to encrypt track data. If the data is properly encrypted in transit and at rest, it shouldn't be of any use to attackers. "This is a breach that should've never happened," Forrester analyst John Kindervag said in an emailed statement. "The fact that three-digit CVV security codes were compromised shows they were being stored. Storing CVV codes has long been banned by the card brands and the PCI [Security Standards Council]."[23]

41. The Informationweek.com story continues:

> …[A]ttackers may have been able to remotely tap into the POS terminals by exploiting vulnerabilities in their built-in Web servers, Bala Venkat, the chief marketing officer for Web application security vendor Cenzic, said in an emailed statement. "When searching for vulnerable targets, attackers are discovering that many retail merchants and point-of-sale terminals haven't implemented some of the basic security measures required by [PCI]," he said, which would include two-factor authentication on the terminals for anyone attempting to remotely connect to it.
>
> The breach was likely compounded by Target failing to monitor its POS terminals for signs of attack. "This seems rather obvious from the information revealed already about this Target breach," Venkat said.[24]

---

[21] http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/.

[22] http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/.

[23] http://www.informationweek.com/security/attacks-and-breaches/target-breach-10-facts/d/d-id/1113228.

[24] *Id*.

42. Thieves could not have accessed Target's network and stolen consumers' credit card, ATM/debit card and personal information but for Target's inadequate security protections. Target failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information that was compromised.

43. Despite the risk posed to consumers, Target did not immediately notify its customers of the breach. Target chose to release a statement on its corporate website; not target.com, the shopping website regularly accessed by consumers. Additionally, in its December 19, 2013, statement, Target also claimed to "have worked swiftly to resolve the incident," and downplayed the threat to consumers by assuring that "[t]here is no indication that PIN numbers have been compromised on affected bank issued PIN debit cards or Target debit cards" and that the CVV codes that were stolen are not the same as the three-digit security code on the back of consumers' cards.[25] These claims by Target imparted a false sense of security to affected consumers. Target also downplayed the risk, urging consumers to merely "check [their] account for any suspicious or unusual activity."

44. Target's failure to promptly and effectively inform customers earlier of the data theft left an untold number vulnerable to attack.

45. Despite advising Target customers who used a Target branded REDcard to "contact Target" if something "appears fraudulent," many customers reported that they were unable to ascertain whether their card was impacted because Target's REDcard website repeatedly timed out and the consumer toll-free number was inundated by complaints, making it impossible to check if any fraudulent charges had been made.[26]

46. Although Target is not disclosing exactly how the breach occurred, industry experts have speculated on how the breach occurred. Ken Stasiak, founder and CEO of Secure State, a Cleveland-based information security firm that investigates data breaches like this one suspected that this breach was perpetrated by organized crime. Stasiak's theory is that the hackers were able to breach Target's main information hub and then wrote a code that gave them access to the

[25] https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5880.

[26] http://www.cbsnews.com/news/customers-seeing-red-over-targets-hacking-response/.

company's POS system and all of its cash registers. That access allowed the attackers to capture the data from shoppers' cards as they were swiped. Independent research into the sale of the personal and financial information revealed that the proprietor of the online store selling the information on the black market is likely located in Russia.[27]

47. Similarly, James Lyne, global head of security research for the computer security firm Sophos, says something clearly went wrong with Target's security measures. "Forty million cards stolen really shows a substantial security failure," he says. "This shouldn't have happened."[28]

**D. The Data Breach Harmed Plaintiff and Other Class Members**

48. As a result of Target's unfair, inadequate, and unreasonable data security, cyber-criminals now possess the personal and financial information of Plaintiffs and the Class. While credit card companies offer protection against unauthorized chargers, the process is long, costly, and frustrating. Physical cards must be replaced, credit card information must be updated on all automatic payment accounts, and victims must add themselves to credit fraud watch lists, which substantially impair victims' ability to obtain additional credit. As Target now admits that names, addresses, phone numbers and email addresses were also stolen, there is a real and compounding risk that Plaintiffs and the Class will be victims of identity theft. Compounding the injury to Plaintiffs and the Class is the fact that their personal and financial information was stolen during the height of holiday shopping and travel season when consumers are in particular need of their cards.

49. Immediate notice of the breach is essential to obtain the best protection afforded by identity theft protection services. Target failed to provide such immediate notice, thus further exacerbating the damages sustained by Plaintiffs and the Class resulting from the breach.

50. Personal and financial information is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen credit card numbers, Social Security numbers, and other personal information on a number of Internet websites.

---

[27] http://krebsonsecurity.com/2013/12/whos-selling-credit-cards-from-target/.

[28] http://abcnews.go.com/Business/wireStory/answers-questions-target-data-breach-21277703

51. The personal and financial information that Target failed to adequately protect, including Plaintiffs identifying information, is "as good as gold" to identity thieves because identity thieves can use victims' personal data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

52. Plaintiffs' and Class members' personal and financial information stolen from Target flooded the underground black markets with batches of one million card numbers selling from $20 to $100 per card.[29] The online black markets also provided purchasing thieves with the zip code and location of the Target store where the information was stolen.[30] This allowed thieves to make same-state purchases, thus avoiding any blocks from banks who suspect fraud.

53. Although Target ultimately offered free credit monitoring to some customers, the credit monitoring services do nothing to prevent credit card fraud. Credit monitoring only informs a consumer of instances of fraudulent opening of new accounts, not fraudulent use of existing credit cards. Thus, Plaintiffs and the Class must take additional steps to protect their credit as described above.

## V. CLASS ALLEGATIONS

54. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action as a national class action for themselves and all members of the following Class of similarly situated individuals and entities:

**The Class**

> All persons and entities in the United States who used a credit or debit card at Target stores and whose personal and financial information was compromised as a result of the data breach first disclosed by Target on December 19, 2013.

55. Excluded from the Class are Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as

[29] http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/.

[30] *Id.*

the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant.

56. Plaintiffs also seek to certify the following Subclasses of the Class:

**The California Subclass**

All members of the Class who are residents of California.

**The Colorado Subclass**

All members of the Class who are residents of Colorado.

**The Washington Subclass**

All members of the Class who are residents of Washington.

**The Arizona Subclass**

All members of the Class who are residents of Arizona.

Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleged the same claims.

57. ***Numerosity***. The Class is so numerous that joinder of all members is unfeasible and not practical. While the precise number of Class members has not been determined at this time, Target has admitted that 40 million credit and ATM card accounts and PINs were stolen and as many as 70 million persons had their personal information compromised in the data breach that Target first disclosed on December 19, 2013.

58. ***Commonality***. Questions of law and fact common to all Class members exist and predominate over any questions affecting only individual Class members, including, *inter alia*:

a. whether Target engaged in the wrongful conduct alleged herein;

b. whether Target's conduct was deceptive, unfair, and/or unlawful;

c. whether Target's conduct was likely to deceive a reasonable person;

d. whether Target used reasonable and industry-standard safety measures to protect Class members, personal and financial information;

e. whether Target knew or should have known that its POS system was vulnerable to attack;

f. whether Target violated California Business and Professions Code § 17200, *et. seq.*;

g. Whether Target, a Minnesota Corporation, complied with Minnesota laws concerning consumer protection and data breach disclosures;

h. whether Target violated the Colorado Consumer Protection Act;

i. whether Target violated the Arizona Consumer Fraud Act;

j. whether Target violated the Washington Unfair Competition Law;

k. whether Target violated the New Hampshire Consumer Protection Act;

l. whether Plaintiffs and Class members are entitled to recover actual damages, statutory damages, and/or punitive damages; and

m. whether Plaintiffs and Class members are entitled to restitution, disgorgement, and/or other equitable relief.

59. ***Typicality***. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all Class members were injured through the uniform misconduct described above and assert the same claims for relief.

60. ***Adequacy***. Plaintiffs and their counsel will fairly and adequately represent the interests of the Class members. Plaintiffs have no interests antagonistic to, or in conflict with, the interests of the Class members. Plaintiffs' lawyers are highly experienced in the prosecution of consumer class actions and complex commercial litigation.

61. ***Superiority***. A class action is superior to all other available methods for fairly and efficiently adjudicating the claims of Plaintiffs and the Class members. Plaintiffs and the Class members have been harmed by Target's wrongful actions and/or inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Target's wrongful actions and/or inaction.

62. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

63. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2) because Target has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

64. The expense and burden of litigation would substantially impair the ability of Plaintiffs and Class members to pursue individual lawsuits to vindicate their rights. Absent a class action, Target will retain the benefits of its wrongdoing despite its serious violations of the law.

## VI. COUNTS

### COUNT I

### NEGLIGENCE

### (On Behalf of All Plaintiffs and the Class)

65. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

66. By accepting Plaintiffs' and Class members' non-public personal and financial information, Target assumed a duty requiring it to use reasonable and industry standard care to secure such information against theft and misuse.

67. Target breached its duty of care by failing to adequately secure and protect Plaintiffs' and the Class members' personal and financial information from theft, collection and misuse by third parties.

68. Target further breached its duty of care by failing to promptly, clearly, accurately, and completely inform Plaintiffs and the Class that their personal and financial information had been stolen.

69. Plaintiffs and the Class have suffered injury in fact, including monetary damages, and will continue to be injured and incur damages as a result of Target's negligence and misconduct.

70. As a direct and proximate result of Target's failure to take reasonable care and use industry standard measures to protect the personal and financial information placed in its care, Plaintiffs and members of the Class had their personal and financial information stolen, causing

direct and measurable monetary losses, threat of future losses, identity theft and threat of identity theft.

71. As a direct and proximate result of Target's negligence and misconduct, Plaintiffs and the Class were injured in fact by: (a) unauthorized charges on their debit and credit card accounts; (b) theft of their personal and financial information; (c) costs associated with the detection and prevention of identity theft; (d) costs associated with the detection and prevention of unauthorized use of their financial accounts; (e) costs associated with being unable to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts; and (f) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the POS data breach, all of which have an ascertainable monetary value to be proven at trial.

**COUNT II**

**VIOLATION OF MINNESOTA STAT. 325E.61**

**(On Behalf of All Plaintiffs and the Class)**

72. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

73. Target is a Minnesota Corporation.

74. The Minnesota Private Attorney General Act permits a private cause of action for violations of law "respecting unfair, discriminatory, and other unlawful practices in business, commerce, or trade." MINN. STAT. § 8.31, subd. 1, 3a. Plaintiffs may bring this case under the Private Attorney General Act because adjudication of Plaintiffs' claims will benefit the public. There is a significant public interest in requiring Target to comply with statutes designed to protect consumers from identity and data theft and requiring Target to use reasonable means and industry measures to protect personal and financial information on its computer systems from theft and unauthorized use.

75. Under MINN. STAT. § 325E.61, Minnesota businesses are required to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is

reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay."

76. Target did not disclose or publicly report the POS data breach until it was forced to do so by the Krebs blog and news media reports that followed it. Target's disclosure of the POS data breach was not completed in the most expedient time possible and it was not done without unreasonable delay.

77. Target failed to provide individualized notice to the Class until nearly a month after the POS data breach began, well after Class financial and personal information was being sold and fraudulently used, and at least four days after Target had discovered and terminated the POS data breach. Target's notice, in addition to being unreasonably delayed and untimely was unclear, incomplete, incorrect, and intended to protect its reputation and holiday sales instead of protecting the Class from harm and damages from the POS data breach.

## COUNT III

## VIOLATION OF MINNESOTA DECEPTIVE TRADE PRACTICE ACT
**MINN. STAT. § 325D.43, *et seq.***

**(On Behalf of All Plaintiffs and the Class)**

78. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

79. Target is a Minnesota Corporation.

80. The Minnesota Private Attorney General Act permits a private cause of action for violations the Minnesota Deceptive Trade Practices Act ("DTPA") pursuant to Minn. DTPA §§ 325D.43, *et seq.* and MINN. STAT. § 8.31. Plaintiffs seek to remedy Target's ongoing unlawful, unfair and fraudulent business practices and seek injunctive relief and restitution.

81. Target's acts and omissions affect trade and commerce and affect sponsorship of goods and services in Minnesota.

82. Target has committed acts of unfair competition by representing to Plaintiffs and the Class that personal and financial information provided to Target in sales transactions would be safe and secure from theft and unauthorized use when in truth and fact Target did not take reasonable

and industry standard measures to protect such personal and financial information from theft and misuse. Target has violated MINN. STAT. § 325D.44(5) through its representations that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have…"

83. Target has also violated MINN. STAT. § 325D.44(7) because it represented that its goods and services were of a particular standard, quality or grade, when in truth and fact, they were not.

84. Target conducted the practices alleged herein in the course of its business, pursuant to standardized practices that it engaged in both before and after the Plaintiffs in this case were harmed, these acts have been repeated millions of times, and many consumers were affected.

85. Target's misrepresentations and omissions were material to Plaintiffs' and the Class' transactions with Target and were made knowingly and with reason to know that Plaintiffs and the Class would rely on the misrepresentations and omissions.

86. Plaintiffs and the Class reasonably relied on Target's misrepresentations and omissions and suffered harm as a result, including: (a) unauthorized charges on their debit and credit card accounts; (b) theft of their personal and financial information; (c) costs associated with the detection and prevention of identity theft; (d) costs associated with the detection and prevention of unauthorized use of their financial accounts; (e) costs associated with being unable to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts; and (f) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the POS data breach, all of which have an ascertainable monetary value to be proven at trial.

87. Target's acts and practices described herein are "fraudulent" under the DTPA because they are likely to deceive the public and affect consumers' legal rights and obligations and through its deception, concealment and falsity, Target may preclude consumers from exercising legal rights to which they are entitled.

**COUNT IV**

**VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL")**
**CAL. BUS. & PROF. CODE § 17200, *et seq.***

**(On Behalf of Plaintiff Mancias and the California Subclass)**

88. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

89. Target engaged in unfair, unlawful, and fraudulent business practices in violation of the UCL.

90. California Business & Professions Code § 17200 prohibits any "unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." For the reasons discussed above, Target violated (and, on information and belief, continues to violate) California Business & Professions Code § 17200 by engaging in the above-described and prohibited unlawful, unfair, fraudulent, deceptive, untrue, and misleading acts and practices.

91. Target violated the UCL by accepting and storing Plaintiffs' and the Class members' personal and financial information but failing to take reasonable steps to protect it. In violation of industry standards and best practices, Target also violated consumer expectations to safeguard personal and financial information and failed to tell consumers that it did not have reasonable and best practices, safeguards and data security in place.

92. Target also violated the UCL by failing to immediately notify Plaintiffs and the Class of the POS data breach. If Plaintiffs and the Class had been notified in an appropriate fashion, they could have taken precautions to better safeguard their personal and financial information.

93. Target's above-described wrongful acts and practices also constitute "unlawful" business acts and practices in violation of California's fraud and deceit statutes, CIVIL CODE §§ 1572, 1573, 1709, 1711, California's Data Breach Act, CIVIL CODE §1798.80, *et seq.*, BUSINESS & PROFESSIONS CODE §§ 17200, *et seq.*, §§ 17500, *et seq.*, and the common law.

94. Target's above-described wrongful acts and practices also constitute "unfair" business acts and practices, in that the harm caused by Target's above wrongful conduct outweighs

any utility of such conduct, and such conduct (i) offends public policy, (ii) is immoral, unscrupulous, unethical, oppressive, deceitful and offensive, and/or (iii) has caused (and will continue to cause) substantial injury to consumers, such as Plaintiffs and the Class. There were reasonably available alternatives to further Target's legitimate business interests, including using best practices to protect the personal and financial information, other than Target's wrongful conduct described herein.

95. Plaintiffs allege violations of California consumer protection and unfair competition laws resulting in harm to consumers. Plaintiffs assert violations of public policy against engaging in unfair competition, and deceptive conduct towards consumers. This conduct also constitutes violations of the "unfair" prong of California Business and Professions Code § 17200.

96. On information and belief, Target's unlawful, fraudulent, and unfair business acts and practices, except as otherwise indicated herein, continue to this day and are ongoing. As a direct and/or proximate result of Target's unlawful, unfair, and fraudulent practices, Plaintiffs and the Class have suffered injury in fact and lost money in connection with their credit or debit purchases at Target stores during the time of the data breach, for which they are entitled to compensation – as well as restitution, disgorgement, and/or other equitable relief.

97. Plaintiffs, for themselves and the Class, also are entitled to injunctive relief, under California Business and Professions Code §§ 17203, 17204, to stop Target's above-described wrongful acts and practices and require Target to maintain adequate or reasonable security measures to protect the personal and financial information in its possession or, in the alternative, for restitution and/or disgorgement.

## COUNT V

## VIOLATION OF CALIFORNIA DATA BREACH ACT
**CAL. CIV. CODE § 1798.80, *et seq.***

**(On Behalf of Plaintiff Mancias and the California Subclass)**

98. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

99. Section 1798.82 of the CALIFORNIA CIVIL CODE provides, in pertinent part, as follows:

> (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
>
> (b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
>
> (c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.
>
> (d) Any person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:
>
> (1) The security breach notification shall be written in plain language.
>
> (2) The security breach notification shall include, at a minimum, the following information:
>
> (A) The name and contact information of the reporting person or business subject to this section.
>
> (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
>
> (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.
>
> (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

* * *

(f) Any person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

100. The POS data breach constituted a "breach of the security system" of Target.

101. Plaintiffs' names, credit and debit card numbers, card expiration dates, CVVs, addresses, phone numbers and email addresses constitute "personal information."

102. Target unreasonably delayed in informing anyone about the breach of security of Class members' confidential and non-public information after Target knew the data breach had occurred.

103. Target failed to disclose to Class members without unreasonable delay and in the most expedient time possible, the breach of security of consumers' personal and financial information when they knew or reasonably believed such information had been compromised.

104. Upon information and belief, no law enforcement agency instructed Target that notification to Class members would impede investigation.

105. Pursuant to Section 1798.84 of the CALIFORNIA CIVIL CODE:

(a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.

> (b) Any customer injured by a violation of this title may institute a civil action to recover damages.
>
> (c) In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars ($3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars ($500) per violation for a violation of Section 1798.83.
>
> * * *
>
> (e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

106. Plaintiffs individually and on behalf of the Class seek all remedies available under CAL. CIV. CODE § 1798.84, including, but not limited to: (a) damages suffered by Class members as alleged above; (b) statutory damages for Target's willful, intentional, and/or reckless violation of CAL. CIV. CODE § 1798.83; and (c) equitable relief.

107. Plaintiffs on behalf of themselves and the Class also seek reasonable attorneys' fees and costs under CAL. CIV. CODE § 1798.84(g).

**COUNT VI**

**VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT**

**(On Behalf of Plaintiffs Lawhern and Del Nagro and the Washington Subclass)**

108. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

109. The conduct of Defendant as set forth herein constitutes unfair or deceptive acts or practices, including, but not limited to accepting and storing Plaintiffs' and the Class members' personal and financial information but failing to take reasonable steps to protect it. In violation of industry standards and best practices, Target also violated consumer expectations to safeguard personal and financial information and failed to tell consumers that it did not have reasonable and best practices, safeguards and data security in place.

110. Target also violated the Washington Consumer Protection Act by failing to immediately notify Plaintiffs and the Class of the POS data breach. If Plaintiffs and the Class had been notified in an appropriate fashion, they could have taken precautions to better safeguard their personal and financial information.

111. Defendant's actions as set forth above occurred in the conduct of trade or commerce.

112. To establish that an act is a "consumer" transaction it must be likely that "additional plaintiffs have been or will be injured in exactly the same fashion." *Hangman Ridge Training Stables, Inc. v. Safeco Title Ins. Co.*, 105 Wn.2d 778, 790 (1986).

113. Plaintiffs were injured exactly the same way as millions of other Target customers. In a consumer transaction, the following factors determine whether the transaction "impacts the public interest":

> (1) Were the alleged acts committed in the course of defendant's business? (2) Are the acts part of a pattern or generalized course of conduct? (3) Were repeated acts committed prior to the act involving plaintiff? (4) Is there a real and substantial potential for repetition of defendant's conduct after the act involving plaintiff? (5) If the act complained of involved a single transaction, were many consumers affected or likely to be affected by it?

*Id*.

114. Defendant conducted the practices alleged herein in the course of its business, pursuant to standardized practices that it engaged in both before and after the Plaintiffs in this case were harmed, these acts have been repeated millions of times, and many consumers were affected.

115. As a direct and proximate result of Target's negligence and misconduct described in this complaint, Plaintiffs and the Class were injured in fact by: (a) unauthorized charges on their debit and credit card accounts; (b) theft of their personal and financial information; (c) costs associated with the detection and prevention of identity theft; (d) costs associated with the detection and prevention of unauthorized use of their financial accounts; (e) costs associated with being unable to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts; and (f) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the POS data breach, all of which have an ascertainable monetary value to be proven at trial.

116. Defendant's conduct proximately caused Plaintiffs' and the Class's injuries.

117. Defendant is liable to Plaintiffs and the Class for damages in amounts to be proven at trial, including attorneys' fees, costs, and treble damages.

**COUNT VII**

**VIOLATION OF THE ARIZONA CONSUMER FRAUD ACT**

**(On Behalf of Plaintiff Davis and the Arizona Subclass)**

118. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

119. Target's publicly disclosed privacy policy and website made use of deception, false promises, misrepresentations and material omissions in connection with the sale and advertisement of its merchandise and services, in violation of the Arizona Consumer Fraud Act, ARIZ. REV. STAT. § 44-1522(A).

120. Target's false, deceptive and misleading statements, and/or omissions of material facts, were made with the intent that consumer rely on such concealment, suppression or omission, in connection with the sale and advertisement of merchandise and services.

121. Target used false, deceptive and misleading statements, and omitted material facts, concerning the scope of its security and safeguards for consumers' personal and financial information which it collected and stored on its POS computer systems. Target led consumers to believe that their personal and financial information was secure and safe from theft, when in reality Target had not implemented reasonable and industry methods to prevent the theft of consumer personal and financial information.

122. Target also used false, deceptive and misleading statements, and omitted material facts, concerning the POS data breach when it ultimately disclosed it had occurred and in the months and weeks thereafter, as more fully described above.

**COUNT VIII**

**VIOLATION OF THE COLORADO CONSUMER PROTECTION ACT**

**(On Behalf of Plaintiff Abels and the Colorado Subclass)**

123. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs.

124. Target's publicly disclosed privacy policy and website made use of deception, false promises, misrepresentations and material omissions in connection with the sale and advertisement

of its merchandise and services, in violation of the Colorado Consumer Protection Act, COLO. REV. STAT. § 6-1-105(1).

125. Target's false, deceptive and misleading statements, and/or omissions of material facts, were made with the intent that consumers rely on such concealment, suppression or omission, in connection with the sale and advertisement of merchandise and services.

126. Target used false, deceptive and misleading statements, and omitted material facts, concerning the scope of its security and safeguards for consumers' personal and financial information which it collected and stored on its POS computer systems. Target led consumers to believe that their personal and financial information was secure and safe from theft, when in reality Target had not implemented reasonable and industry methods to prevent the theft of consumer personal and financial information.

127. Target also violated the Consumer protection Act, COLO. REV. STAT. § 6-1-105(1)(x), through its violation of COLO. REV. STAT. § 6-1-716 by failing to timely, accurately, and completely disclose the facts concerning the POS data breach. Plaintiff Abels and the Colorado Subclass are entitled to statutory damages, if applicable. COLO. REV. STAT. § 6-1-113.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request the following relief:

A. That the Court certify this case as a class action and appoint the named Plaintiffs to be Class representatives and their counsel to be Class counsel;

B. That the Court award Plaintiffs appropriate relief, to include actual and statutory damages, disgorgement, and restitution;

C. That the Court award Plaintiffs preliminary or other equitable or declaratory relief as may be appropriate by way of applicable state or federal law;

D. Such additional orders or judgments as may be necessary to prevent these practices and to restore to any person in interest any money or property which may have been acquired by means of the violations; and

E. That the Court award Plaintiffs such other, favorable relief as may be available and appropriate under law or at equity.

**JURY TRIAL DEMANDED**

Plaintiffs demand a trial by jury on all issues so triable.

DATED: January 14, 2014

HAGENS BERMAN SOBOL SHAPIRO LLP

By /s/ *Thomas E. Loeser*
Thomas E. Loeser (202724)

Steve W. Berman, *pro hac vice* (application pending)
Thomas E. Loeser (202724)
HAGENS BERMAN SOBOL SHAPIRO LLP
1918 Eighth Avenue, Suite 3300
Seattle, WA 98101
Telephone: (206) 623-7292
Facsimile: (206) 623-0594
steve@hbsslaw.com
toml@hbsslaw.com

Jeff D. Friedman (173886)
HAGENS BERMAN SOBOL SHAPIRO LLP
715 Hearst Avenue, Suite 202
Berkeley, CA 94710
Telephone: (510) 725-3000
Facsimile: (510) 725-3001
jefff@hbsslaw.com

*Attorneys for Plaintiffs and the Proposed Class*